An Attack to Quantum Cryptography from Space

Igor V. Volovich*

Department of Mathematics, Statistics and Computer Sciences
University of Vaxjo, S-35195, Sweden

Abstract

The promise of secure cryptographic quantum key distribution schemes is based on the use of quantum effects in the spin space. We point out that in fact in many current quantum cryptography protocols the space part of the wave function is neglected. However exactly the space part of the wave function describes the behaviour of particles in ordinary real three-dimensional space. As a result such schemes can be secure against eavesdropping attacks in the abstract spin space but could be insecure in the real three-dimensional space. We discuss an approach to the security of quantum key distribution in space by using Bell's inequality and a special preparation of the space part of the wave function.

*Permanent address: Steklov Mathematical Institute, Gubkin St.8, GSP-1, 117966, Moscow, Russia; volovich@mi.ras.ru

1 Introduction

It is now generally accepted that techniques of quantum cryptography can allow secure communications between distant parties [1] - [14]. The promise of secure cryptographic quantum key distribution schemes is based on the use of quantum entanglement in the spin space and on quantum no-cloning theorem. An important contribution of quantum cryptography is a mechanism for detecting eavesdropping.

In the present note we point out that in fact in many current quantum cryptography protocols the space part of the wave function is neglected. However exactly the space part of the wave function describes the behaviour of particles in ordinary real three-dimensional space. As a result such schemes can be secure against eavesdropping attacks in the abstract spin space but could be insecure in the real three-dimensional space. We discuss an approach to the security of quantum key distribution in the real space by using Bell's inequality and a special preparation of the space part of the wave function.

Bell's theorem [15] states that there are quantum correlation functions that can not be represented as classical correlation functions of separated random variables. It has been interpreted as incompatibility of the requirement of locality with the statistical predictions of quantum mechanics [15]. Bell's theorem constitutes an important part in quantum cryptography protocols [2].

It was mentioned in [16] that the space dependence of the wave function is neglected in discussions of the problem of locality in relation to Bell's inequalities. However it is the space part of the wave function which is relevant to the consideration of the problem of locality. Similar remark one can apply to quantum teleportation [17]. It was shown [16] that the space part of the wave function leads to an extra factor in quantum correlation and as a result the ordinary proof of Bell's theorem fails in this case.

It follows that proofs of the security of quantum cryptography schemes which neglect the space part of the wave function could fail against attacks in the real three-dimensional space. We will discuss how one can try to improve the security of quantum cryptography schemes in space by using a special preparation of the space part of the wave function.

2 Quantum Key Distribution

Ekert [2] showed that one can use the EPR correlations to establish a secret random key between two parties ("Alice" and "Bob"). Bell's inequalities are used to check the presence of an intermediate eavesdropper ("Eve"). There are two stages to the Ekert protocol, the first stage over a quantum channel, the second over a public channel.

The quantum channel consists of a source that emits pairs of spin one-half particles, in a singlet state. The particles fly apart towards Alice and Bob, who, after the particles have separated, perform measurements on spin components along one of three directions, given by unit vectors a and b. In the second stage Alice and Bob communicate over a public channel.They announce in public the orientation of the detectors they have chosen for particular measurements. Then they divide the measurement results into two separate groups: a first group for which they used different orientation of the detectors, and a second group for which they used the same orientation of the detectors. Now Alice and Bob can reveal publicly the results they obtained but within the first group of measurements only. This allows them, by using Bell's inequality, to establish the presence of an eavesdropper (Eve). The results of the second group of measurements can be converted into a secret key.

3 Bell's Inequality

In the presentation of Bell's theorem we will follow [16] where one can find also more references. Consider a pair of spin one-half particles formed in the singlet spin state and moving freely towards Alice and Bob. If one neglects the space part of the wave function then the quantum mechanical correlation of two spins in the singlet state ψ_{spin} is

$$E_{spin}(a,b) = \langle \psi_{spin} | \sigma \cdot a \otimes \sigma \cdot b | \psi_{spin} \rangle = -a \cdot b \tag{1}$$

Here a and b are two unit vectors in three-dimensional space and $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli matrices. Bell's theorem states that the function $E_{spin}(a,b)$ (1) can not be represented in the form

$$P(a,b) = \int \xi(a,\lambda)\eta(b,\lambda)d\rho(\lambda) \tag{2}$$

Here $\xi(a,\lambda)$ and $\eta(b,\lambda)$ are random fields on the sphere, $|\xi(a,\lambda)| \leq 1$, $|\eta(b,\lambda)| \leq 1$ and $d\rho(\lambda)$ is a positive probability measure, $\int d\rho(\lambda) = 1$. The parameters λ are interpreted as hidden variables in a realist theory. One supposes that Eve is described by these variables.

One has the following Bell-Clauser-Horn-Shimony-Holt (CHSH) inequality

$$|P(a,b) - P(a,b') + P(a',b) + P(a',b')| \leq 2 \tag{3}$$

From the other hand there are such vectors ($ab = a'b = a'b' = -ab' = \sqrt{2}/2$) for which one has

$$|E_{spin}(a,b) - E_{spin}(a,b') + E_{spin}(a',b) + E_{spin}(a',b')| = 2\sqrt{2} \tag{4}$$

Therefore if one supposes that $E_{spin}(a,b) = P(a,b)$ then one gets the contradiction.

4 Localized Detectors

In the previous section the space part of the wave function of the particles was neglected. However exactly the space part is relevant to the discussion of locality. The complete wave function is $\psi = (\psi_{\alpha\beta}(\mathbf{r}_1,\mathbf{r}_2))$ where α and β are spinor indices and $\mathbf{r}_1$ and $\mathbf{r}_2$ are vectors in three-dimensional space.

We suppose that Alice and Bob have detectors which are located within the two localized regions $\mathcal{O}_A$ and $\mathcal{O}_B$ respectively, well separated from one another. Eve has a detector which is located within the region $\mathcal{O}_E$. Quantum correlation describing the measurements of spins by Alice and Bob at their localized detectors is

$$E(a,\mathcal{O}_A,b,\mathcal{O}_B) = \langle\psi|\sigma\cdot aP_{\mathcal{O}_A} \otimes \sigma\cdot bP_{\mathcal{O}_B}|\psi\rangle \tag{5}$$

Here $P_{\mathcal{O}}$ is the projection operator onto the region $\mathcal{O}$.

Let us consider the case when the wave function has the form $\psi = \psi_{spin}\phi(\mathbf{r}_1,\mathbf{r}_2)$. Then one has

$$E(a,\mathcal{O}_A,b,\mathcal{O}_B) = g(\mathcal{O}_A,\mathcal{O}_B)E_{spin}(a,b) \tag{6}$$

where the function

$$g(\mathcal{O}_A,\mathcal{O}_B) = \int_{\mathcal{O}_A\times\mathcal{O}_B} |\phi(\mathbf{r}_1,\mathbf{r}_2)|^2 d\mathbf{r}_1 d\mathbf{r}_2 \tag{7}$$

describes correlation of particles in space. Note that one has

$$0 \leq g(\mathcal{O}_A, \mathcal{O}_B) \leq 1 \tag{8}$$

Remark. In relativistic quantum field theory there is no nonzero strictly localized projection operator that annihilates the vacuum. It is a consequence of the Reeh-Schlieder theorem [18]. Therefore, apparently, the function $g(\mathcal{O}_A, \mathcal{O}_B)$ should be always strictly smaller than 1. I am grateful to W. Luecke for this remark.

We will interpret Eve as a hidden variable in a realist theory and will study whether the quantum correlation (6) can be represented in the form (2). More exactly one inquires whether one can write the representation

$$g(\mathcal{O}_A, \mathcal{O}_B) E_{spin}(a, b) = \int \xi(a, \mathcal{O}_A, \lambda) \eta(b, \mathcal{O}_B, \lambda) d\rho(\lambda) \tag{9}$$

Now from (3), (4) and (9) one can obtain the following inequality

$$g(\mathcal{O}_A, \mathcal{O}_B) \leq 1/\sqrt{2} \tag{10}$$

If the inequality (10) is valid for regions $\mathcal{O}_A$ and $\mathcal{O}_B$ which are well separated from one another then there is no violation of the CHSH inequalities (3) and therefore Alice and Bob can not detect the presence of an eavesdropper. From the other side, if for a pair of well separated regions $\mathcal{O}_A$ and $\mathcal{O}_B$ one has

$$g(\mathcal{O}_A, \mathcal{O}_B) > 1/\sqrt{2} \tag{11}$$

then it could be a violation of the realist locality in these regions for a given state. Then, in principle, one can hope to detect an eavesdropper in these circumstances.

Note that if we set $g(\mathcal{O}_A, \mathcal{O}_B) = 1$ in (9) as it was done in the original proof of Bell's theorem, then it means we did a special preparation of the states of particles to be completely localized inside of detectors. There exist such well localized states (see however the previous Remark) but there exist also another states, with the wave functions which are not very well localized inside the detectors, and still particles in such states are also observed in detectors. The fact that a particle is observed inside the detector does not mean, of course, that its wave function is strictly localized inside the detector before the measurement. Actually one has to perform a thorough investigation of the preparation and the evolution of our entangled states in space and time if one needs to estimate the function $g(\mathcal{O}_A, \mathcal{O}_B)$.

5 Conclusions

It is pointed out in this note that the presence of the space part in the wave function of two particles in the entangled state leads to a problem in the proof of the security of quantum key distribution. To detect the eavesdropper's presence by using Bell's inequality we have to estimate the function $g(\mathcal{O}_A, \mathcal{O}_B)$. Only a special quantum key distribution protocol has been discussed here but it seems there are similar problems in other quantum cryptographic schemes as well.

We don't claim in this note that it is in principle impossible to increase the detectability of the eavesdropper. However it is not clear to the present author how to do it without a thorough investigation of the process of preparation of the entangled state and then its evolution in space and time towards Alice and Bob.

In the previous section Eve was interpreted as an abstract hidden variable. However one can assume that more information about Eve is available. In particular one can assume that she is located somewhere in space in a region $\mathcal{O}_E$. It seems one has to study a generalization of the function $g(\mathcal{O}_A, \mathcal{O}_B)$, which depends not only on the Alice and Bob locations $\mathcal{O}_A$ and $\mathcal{O}_B$ but also depends on the Eve location $\mathcal{O}_E$, and try to find a strategy which leads to an optimal value of this function.

6 Acknowledgments

I would like to thank A.Khrennikov and the Department of Mathematics, Statistics and Computer Sciences, University of Vaxjo, where this work was done, for the warm hospitality. I am grateful to J.L. Cereceda, G. Garbarino, S. Goldstein, W. Hofer, W. Luecke, N. D. Mermin, K. Svozil, and P. Zanardi for correspondence on Bell's theorem.

References

[1] C.H. Bennett and G. Brassard, in *Proc. of the IEEE Inst. Conf. on Comuters, Systems, and Signal Processing, Bangalore, India* (IEEE, New York,1984) p.175

[2] A.K. Ekert, Phys. Rev. Lett. 67 (1991)661

[3] Dominic Mayers, Andrew Yao, *Quantum Cryptography with Imperfect Apparatus,* quant-ph/9809039

[4] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, P. G. Kwiat, *Entangled state quantum cryptography: Eavesdropping on the Ekert protocol,* quant-ph/9912105

[5] Gilles Brassard, Norbert Lutkenhaus, Tal Mor, Barry C. Sanders, *Security Aspects of Practical Quantum Cryptography,* quant-ph/9911054

[6] Kei Inoue, Takashi Matsuoka, Masanori Ohya, *New approach to Epsilon-entropy and Its comparison with Kolmogorov's Epsilon-entropy,* quant-ph/9806027

[7] Hoi-Kwong Lo, *Will Quantum Cryptography ever become a successful technology in the marketplace?,* quant-ph/9912011

[8] Horace P. Yuen, *Anonymous-key quantum cryptography and unconditionally secure quantum bit commitment*, quant-ph/0009113

[9] Helle Bechmann-Pasquinucci, Asher Peres, *Quantum cryptography with 3-state systems* , quant-ph/0001083

[10] Akihisa Tomita, Osamu Hirota, *Security of classical noise-based cryptography*, quant-ph/0002044

[11] G. Gilbert, M. Hamrick, *Practical Quantum Cryptography: A Comprehensive Analysis (Part One),* quant-ph/0009027

[12] T. Hirano, T. Konishi, R. Namiki, *Quantum cryptography using balanced homodyne detection,* quant-ph/0008037

[13] Miloslav Dusek, Kamil Bradler, *The effect of multi-pair signal states in quantum cryptography with entangled photons,* quant-ph/0011007

[14] Yong-Sheng Zhang, Chuan-Feng Li, Guang-Can Guo, *Quantum key distribution via quantum encryption,* quant-ph/0011034

[15] J.S. Bell, Physics, **1**, 195 (1964)

[16] Igor V. Volovich, *Bell's Theorem and Locality in Space,* quant-ph/0012010

[17] Igor V. Volovich, *Quantum Teleportation in Space,* (in preparation)

[18] Wolfgang Luecke, *Lecture Notes on Quantum Field Theory,* http://www.pt.tu-clausthal.de /∼aswl/scripts/qft.html, Corollary 2.2.14 on page 62.